Notice of Allowability	Application No.	Applicant(s)	
	09/937,634	BAO ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 04/21/2006*.

2. ☒ The allowed claim(s) is/are *1-46*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/21/2006 has been entered.

2. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Examiner withdraws rejection of claims 1-46 under 35 U.S.C 112-second paragraphs due to correction by the applicant.

5. Claims 1, 11-14, 21-24, 34-37 and 44-46 have been amended.

6. Claims 1-46 are pending.

Response to Arguments

7. Applicant's arguments filed 04/21/2006 have been fully considered and they are persuasive.

Allowable Subject Matter

8. Claims 1-46 are allowed.

9. The following is an examiner's statement of reasons for allowance:

York-Smith discloses encryption method and system by encrypting data into a plurality of control and encrypted data blocks.

Luyster disclose block-ciphering method where each blocks are 128 bits or more.

Dole discloses distributed state random number generator and method for utilizing same.

Holmquist disclose encryption using DES in cipher feedback mode of k bits.

Raike discloses non-deterministic public key encryption system.

However York-Smith, Luyster, Dole, Holmquist, Raike's system and method singly or in combination with each other or other prior arts system and method are in contrast with specific steps of applicant's invention where generating the ith segment key s_i for each corresponding ith data segment (i = 1, 2. . .,) to be encrypted, the ith segment key s_i being generable using a sequence generating function with said cryptographic key k and some accessory data strings as inputs; encrypting the ith data segment using a ciphering function with s_i as the encryption key to form the ith ciphertext segment; and outputting the ith ciphertext segment, and at least a part of said accessory data strings for sending

data to the decrypting party and in light of the specification as recited in **independent claims.**

10. **Dependent claims 2-13, 15-23, 25-36 and 38-46** as being dependent upon Independent claims and having additional allowable features therein.

Conclusion

11. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Please see enclosed PTO-892.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is 571-272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

05/09/2006

AU 2132